MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DIRECTOR, DEFENSE RESEARCH AND ENGINEERING
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTOR, NATIONAL RECONNAISSANCE OFFICE
DIRECTORS OF DOD FIELD ACTIVITIES
CHIEF INFORMATION OFFICERS OF THE MILITARY DEPARTMENTS
DIRECTOR, COMMAND CONTROL, COMMUNICATIONS AND COMPUTER SYSTEMS, JOINT STAFF
CHIEF INFORMATION OFFICERS OF THE DEFENSE AGENCIES
DIRECTOR, INTELLIGENCE COMMUNITY MANAGEMENT STAFF
INTELLIGENCE COMMUNITY CHIEF INFORMATION OFFICER
COMMANDERS OF THE UNIFIED COMBATANT COMMANDS

SUBJECT: Department of Defense (DoD) Chief Information Officer (CIO) Guidance and Policy Memorandum No. 4-8460– Department of Defense Network Policy

The attached Department of Defense and Intelligence Community Enterprise Network guidance and policy is effectively immediately. It establishes policies and assigns responsibilities to further achieve effective, efficient, and economical acquisition, management, and use of network equipment and services.

The DoD CIO Executive Board will be the centerpiece for achieving our enterprise-wide network objectives.

This G&PM provides high level policy for immediate implementation. It will also be used to develop future directives and instructions which will replace DoD Directive 4640.13, “ Management of Base and Long-Haul Telecommunications Equipment and Services,” December 5, 1991, and DoD Instruction 4640.14, “Base and Long-Haul Telecommunications Equipment and Services,” December 6, 1991. In the event of conflict, this G&PM takes precedence over DoD Directive 4640.13, “ Management of Base and Long-Haul Telecommunications Equipment and Services,” December 5, 1991.

My point of contact for this effort is COL Neil Putz who can be reached at (703) 607-0466 or by e-mail: neil.putz@osd.pentagon.mil.

<signature block for John Hamre>

Guidance and Policy for the Department of Defense and Intelligence Community Enterprise Network

References: See enclosure 1.

1. PURPOSE

Information superiority for the warfighter, policy maker, and functional user is a critical goal of the DoD. To attain that goal, this issuance establishes policies and guidance, and assigns responsibilities to:

Ensure effective, efficient, and economical acquisition, life-cycle_management, and use of network equipment and services.

Ensure the required security, information assurance, interoperability, and quality are established and maintained in the telecommunications portions of information systems, consistent with the needs of associated missions.

Empower DoD Components to collaboratively create a set of enterprise architectures, practices, and processes, all of which incorporate best practices.

Ensure that Commander-in-Chief (CINC) and Joint Task Force (JTF) policies dominate the allocation and control of warfighter network assets into and within assigned Areas of Responsibility (AOR).

This G&PM provides high level policy for immediate implementation. It will also be used to develop future directives and instructions which will replace references a and b above.

2. APPLICABILITY and SCOPE

This policy guidance applies to:`

The Office of the Secretary of Defense (OSD), the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Inspector General of the Department of Defense (IG, DoD), the Defense Agencies, and the DoD Field Activities (hereafter referred to collectively as "the DoD Components").

All telecommunications equipment and services (including telecommunications components embedded in information systems and contractor-acquired telecommunications) that are administered, managed, acquired, operated or used by the DoD Components.

Implementation of this policy must comply with laws and established DoD and Director Central Intelligence (DCI) Directives relative to architecture, acquisition and security policies and practices.

3. **DEFINITIONS** (See enclosure (1))

4. POLICY

Network Selection Constraints. The DoD CIO Executive Board (see governance section 4.7) will designate a select set of service and transport networks as part of the DoD/IC Enterprise Network. The DoD CIO Executive Board will also identify the organization responsible for program management, configuration management, and property accountability of each service and transport network designated as part of the DoD/IC Enterprise Network. To foster the establishment of a global information grid, all electrical/optical information exchange in support of DoD Components must occur over these designated Enterprise Service and Transport Networks, unless waived in accordance with the provisions in the next section. Taking into account operational requirements and best business practices, the DoD CIO Executive Board will grant waivers for implementation and use of all other service or transport networks. The Intelligence Community Chief Information Office (IC CIO), will establish a sub-group to perform these functions on service and transport networks accredited for Sensitive Compartmented Information (SCI), under the auspices of the IC CIO Executive Council

Architecture. Under the leadership of the Defense Information Systems Agency (DISA), the DoD Components will collaboratively develop an Enterprise-Wide Network Architecture (EWNA) that provides the conceptual foundation, technical guidance, and implementation strategy for the DoD/IC Enterprise Network implementations. The EWNA will encompass strategic and tactical systems architectures and will comply with the DoD Architecture Framework (reference (e)) and required by Clinger-Cohen Act of 1996 (reference (f)), be coordinated through the Architecture Coordination Council, approved by the DoD CIO Executive Board, and maintained by DISA. Security, information assurance, and interoperability are critical parts of the EWNA. Compliance with the EWNA is mandatory, unless waived. The DoD CIO Executive Board is responsible for waiving adherence to the EWNA. The IC CIO will lead the collaborative development and maintenance of the Enterprise-Wide Network Architecture related to SCI networks and will assure appropriate integration with the DISA-led efforts.

Security and Information Assurance. Network managers and providers must provide each other sufficient end-to-end visibility to allow them to meet security and information assurance requirements. Consistent with references (c) and (d), a collaborative approach for certifying and accrediting networks and their interconnections and for extending visibility to network providers and users will be established. For SCI networks, the IC CIO will direct the review and approval of all security and information assurance considerations consistent with DCI policies.

Network Operations. For the purpose of providing security, information assurance and effective management, each Enterprise Service and Transport Network must be managed end-to-end. Network operations policy, to include the concepts of network management, control and visibility of networks and systems end-to-end, will be addressed in a separate policy memorandum.

Performance. To ensure that the DoD/IC Enterprise Network is being deployed and used effectively and efficiently, DoD Components, under the auspices of the DoD CIO Executive Board, will collaboratively develop and implement a uniform evaluation process that defines mechanisms to ensure performance accountability. The process will include the collection and reporting of performance metrics on networks, providers, managers, and users. The IC CIO will lead a similar collaborative effort within the IC for SCI Enterprise Service and Transport Networks.

Financial. The DoD funding strategies for the DoD/IC Enterprise Network will reflect the cost of providing a global enterprise capability that meets requirements (e.g., security, end-to-end visibility, control, interoperability, availability, surge, restoration and reconstitution). The funding strategies will be designed to encourage the use of the enterprise capability and make users fiscally responsible for their use of the network. Users will promptly reconcile their telecommunications invoices._Funding strategy will be addressed under a separate policy memorandum. Funding strategies, which include contributions by DoD Components, will require formal review by the DoD CIO Executive Board. Issues of common concern will be addressed by established DoD and IC boards of jurisdiction.

Governance

Governance of the DoD/IC Enterprise Network is provided by the DoD CIO Executive Board and IC CIO Executive Council (see reference (g) and (h)).

Key responsibilities of the DoD CIO Executive Board are:

Designate a select set of service and transport networks as part of the DoD/IC Enterprise Network, and identify the organization responsible for program management of each service and transport network so designated.

Develop criteria for and_grant waivers for implementation and use of service or transport networks that are not part of the DoD/IC Enterprise Network.

Ensure adherence to EWNA and to grant waivers as appropriate.

Provide annual review to the ASD (C3I)/DoD CIO of the EWNA.

Provide on going coordination with IC CIO council regarding issues of common interest.

For non-resolvable issues between DoD CIO and IC CIO adjudication will be by existing process._ Delete (Any national level resource contentions between military missions and non-military missions are adjudicated at the National Security Council level.)

5. RESPONSIBILITIES

Assistant Secretary of Defense (C3I)/DoD CIO:

Promulgate and ensure compliance with this policy and guidance.

Issue instructions to this policy.

Establish and oversee reporting requirements.

Lead the collaborative development of the DoD CIO Executive Board charter.

Ensure annual review of the effectiveness of the EWNA.

Perform acquisition and procurement oversight of network activities DoD CIO.

Appoint an Executive Agent for Theater Joint Tactical Networks (TJTN).

DoD Executive Board, refer to governance section of this policy.

IC CIO:

The responsibilities of the IC CIO are established in separate DCI Directives and IC CIO Policy Memoranda and are included here only for reference and completeness.

Participate as a member of the DoD CIO Executive Board.

In concert with the DoD CIO Executive Board, designate a select set of networks accredited for SCI for integration with the EWNA and identify organizational responsibility for program management of these SCI networks.

Lead the development of the SCI EWNA and the SCI Enterprise Network evaluation process.

Maintain the EWNA for networks accredited for SCI.

Designate appropriate elements of the IC to participate in the DoD CIO Executive Board.

Review and approve all security and information assurance considerations relative to SCI networks.

Defense Information Systems Agency:

The following responsibilities are established in addition to those identified for all DoD Components below.

Lead the development of the Enterprise-Wide Network Architecture (EWNA).

Coordinate the EWNA through the Architecture Coordination Council.

Maintain the EWNA.

Coordinate with Executive Agency's for Theater Joint Technical Networks (TJTN).

DoD Components/PSAs:

Participate in DoD CIO Executive Board sponsored activities.

Participate in development of EWNA.

Participate in development and implementation of the Enterprise Network evaluation process.

Perform as Enterprise Service Network managers and Enterprise Transport Network providers where designated.

6. EFFECTIVE DATE

This policy is effective immediately upon issuance and until superseded.

Enclosure 1: References

(a) DoD Directive 4640.13, “Management of Base and Long-Haul Telecommunications Equipment and Services,” December 5, 1991

(b) DoD Instruction 4640.14, “Base and Long-Haul Telecommunications Equipment and Services,” December 6, 1991

(c) DoD Directive 5200.28, “Security Requirements for Automated Information Systems (AISs),” March 21, 1998

(d) DCI Directive 6/3, “Security Policy for Uniform Protection of Intelligence Processed on Automated Information Systems and Networks,” June 5, 1999

(e) DoD C4ISR Architecture Framework,” Version 2.0, December 18, 1997

(f) Public Law 104-106, Clinger Cohen Act of 1996, Subdivision E, June 2, 1997

(g) Guidance and Policy Memorandum "Guidance and Policy For the Global Information Grid (GIG) (In progress)

(h) DoD CIO Executive Board Charter (In progress)

Enclosure 2: DEFINITION OF TERMS

E2.1 **EWNA** (Enterprise-Wide Network Architecture): Describes and identifies the DoD/IC Enterprise Network components, their characteristics, and interrelationships necessary to provide the required end-to-end capability. It gives specific network implementation guidance for the wide area (WANs), the regions (MANs), the campuses/facilities (LANs). It includes the specific protocols, enterprise standards, operating profiles, and implementation agreements. It provides the extensive guidance for network services, such as directory, time, and domain name service. It integrates the various Component network architectures (modified by the Components where necessary) into a single, compatible, consistent Enterprise Wide Network Architecture. It also includes a description of DoD/IC Enterprise Network management centers, their functionality, and interrelationships. The security architecture is an integral element of the EWNA and provides specific direction for implementation of a complementary set of security mechanisms to be applied to provide a layered defense for the DoD/IC Enterprise Network. The complete set of EWNA technical tools allows the DoD to set very specific and understandable direction on issues such as interoperability, security, functionality, and performance.

E2.2 **LAN** (Local Area Network): A physical medium and associated equipment that supports the interconnection of computers and peripherals usually over a limited physical area and under a single management control. The LAN demarcation point is the campus, base, post, or station router/switch.

E2.3 **MAN** (Metropolitan Area Network): A system of links or a ring that interconnects a relatively high concentration of LANs together within a small regional area. It is normally used as the means to efficiently connect numerous LANs to each other as well as to a WAN(s). The MAN also provides switching and routing between the LANs as well as between the WAN and the LANs. The demarcation points for the MAN are the service delivery nodes at the campus, base, post, or station router/switch and the hub/router/switch of the WAN.

E2.4 **WAN** (Wide Area Network): A system of links that are used to interconnect geographic regions. The WAN normally provides routing, switching, or gateway points to MANs, LANs, or other WANs.

E2.5 **Transport Network**: A transport network is comprised of any media and associated equipment that is used within DoD/IC to transfer information electronically. These media include, among others, copper wire, fiber optic cable, coaxial cable, satellite transmission systems, radio, and microwave transmission media. The associated equipment include, among others, encryption devices, DSU/CSUs, modems, multiplexers, and switches. When interconnected together, these media and equipment provide the physical path over which information flows.

E2.6 **Service Network**: A service network uses any or all of the transport network elements (LANs, MANs, WANs, and Deployed Systems) and the functionality of routers, switches, gateways, and firewalls, all configured to provide a specified set of capabilities to meet specific user requirements. A service network is operated and managed under a single security policy and set of operating procedures. Examples of service networks are SIPRNET and connected systems, FTS type networks, JWICS and connected systems, NIPRNET and connected systems, DSN and connected systems, Defense Red Switch Network and connected systems, DREN and connected systems, and Navy's SmartLink.

E2.7 **Enterprise Service Network:** A DoD/IC-funded service network which has been designated by the DoD CIO Executive Board as an "Enterprise Service Network" because it: 1) provides a unique, defined capability (e.g., functionality [packet data, switched voice, etc.], security, service assurance, interoperability, network operations, topology, etc.), 2) provides services required by multiple DoD/IC components, 3) is consistent with an established DoD/IC architecture (the Enterprise-Wide Network Architecture, or EWNA), 4) is managed as a single entity, 5) provides service to any user with a validated and funded requirement consistent with the defined capability of that service network

E2.8 **Enterprise Service Network Manager**: For a given Enterprise Service Network, a DoD/IC Component is tasked to manage service end-to-end. The service network manager must coordinate with those transport network providers whose resources are used to provide the end-to-end service.

E2.9 **End-to-end**: End-to-end is defined differently with respect to service networks and transport networks. For service networks, end-to-end encompasses service user to service user (e.g., PC-to-PC, phone-to-phone). For transport networks, end-to-end encompasses equipment-to-equipment (e.g., Service Delivery Point (SDP)-to-Service Delivery Point (SDP), router-to-router, PBX-to-PBX).

E2.10 **Enterprise Transport Network:** A DoD/IC-funded transport network, which has been designated by the DoD CIO Executive Board as an "Enterprise Transport Network" because it provides the underlying capabilities for one or more Enterprise Service Networks. Commercial segments supporting National Security and Emergency Preparedness (NSEP) telecommunications services are subject to Telecommunications Service Priority (TSP) System rules and procedures. The TSP System is the regulatory, administrative, and operational system authorizing priority provision and restoration of NSEP telecommunications services.

E2.11 **Enterprise Transport Network Provider**: For a given Enterprise Transport Network, a DoD/IC Component is tasked to provide connectivity for use by Enterprise Service Networks. The transport network provider must coordinate with those service network managers that use transport network resources.

E2.12 **DoD/IC Enterprise Network**: Comprised of all Service and Transport networks and restoration of NSEP telecommunications services. Designated by the DoD CIO Executive Board as Enterprise Networks, because they: 1) provide a defined capability, 2) are available to serve multiple DoD/IC components, 3) are consistent with an established DoD/IC architecture (the Enterprise-Wide Network Architecture, or EWNA), 4) are managed with enterprise-wide oversight, and 5) provide service to any user with a validated requirement consistent with the defined capability of that service network.

GLOBAL NETWORKED INFORMATION ENTERPRISE (GNIE)

Network Panel Membership

LAST	FIRST	RANK	ORGANIZATION	PHONE	E-MAIL
Harper (Co-chair)	Wayne	GG-15	NRO/NSA/IC	703-808-3181	harperw@nro.mil
Harvey (Co-chair)	Tina	Maj	Joint Staff/J6T	703-693-1747	harveytm@js.pentagon.mil
Bolling	Tom	GS-15	DISA	703-681-0296	bollingt@ncr.disa.mil
Cenac	Jean	CIV	DISA	703-735-8168	cenacj@ncr.disa.mil
Colver	Dick	CIV	ASD(C3I)	703-607-0295	dick.colver@osd.mil
Edelman	Sam	LTC	DISC4	703-614-6166	edelmsl@hqda.army.mil
Edwards	Dave	MITRE	DIA	703-883-7787	edwards@mirte.org
Gaudino	Dick	Col	DISA	703-607-6796	gaudinor@ncr.disa.mil
Henley	John	CIV	DIA		
Ikirt	Steve	Maj	DLA	703-767-6394	steven_ikirt@hq.dla.mil
Johnson	John	CIV	DISA	703-607-6719	johnsonjc@ncr.disa.mil
Kane	Mike	MITRE	MITRE Support	703-883-7920	mkane@mitre.org
Lindholm	Tom		Army Sig Cmd	520-538-7128	lindholmt@hqasc.army.mil
Livengood	Jim	CIV	DLA	703-767-3119	james_livengood@hq.dla.mil
Machado	John	Contractor	Machado Assoc	703-624-4310	machadoj@machadojs.com
Muench	Paul	CIV	NIMA	703-264-2167	nuenchp@nima.mil
Munger	Judy	CIV	DFAS		judy.munger@dfas.mil
Newman	Al	CIV	ASD(C3I)	703-607-0265	al.newman@osd.mil
Payne	Glenn	Lt. Col.	Joint Staff/J6T	703-693-1747	paynegr@js.pentagon.mil
Ramirez	Kim	Civ	Army Sig Cmd	520-538-8679	ramirezk@hqasc.army.mil
Scruggs	Tom	CIV	DON CIO	703-602-6943	scruggs.tom.hq.navy.mil
Shelly	Dave	CIV	AFCIC	703-588-6154	dshelly@af.pentagon.mil
Stack	Larry	CAPT	OPNAC/N6	703-601-1299	stack.lary@hq.navy.mil
Welch	Kim	CIV	DIA	703-	Afwelkr@dia.osis.gov
Woodard	Jim	MSgt	DLA	703-767-6366	james_woodard@hq.dla.mil
Zdeb	Tanya	CIV	AFCIC	703-588-6147	tanya.zdeb@pentagon.mil